

520.1002

9
4

UNITED STATES PATENT & TRADEMARK OFFICE

Re: Application of: **Ulrich HEISTER**
Serial No.: To Be Assigned
Filed: Herewith
For: **DEVICE AND METHOD FOR SYNCHRONIZING
VOLTAGE CIPHERING MACHINE IN ATM
NETWORKS**

LETTER RE: PRIORITY

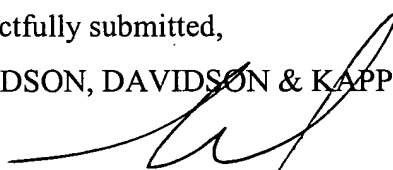
Assistant Commissioner for Patents
Washington, D.C. 20231

July 17, 2001

Sir:

Applicant hereby claims priority of the German Patent Application No. 19901666.6 filed 18 January, 1999 through International Application Serial No. PCT/EP/99/09844, filed December 9, 1999.

Respectfully submitted,
DAVIDSON, DAVIDSON & KAPPEL, LLC

By 
Cary S. Kappel
Reg. No. 36,561

Davidson, Davidson & Kappel, LLC
485 Seventh Avenue, 14th Floor
New York, New York 10018
(212) 736-1940

This Page Blank (uspto)

BUNDESREPUBLIK DEUTSCHLAND

PCT/EP 99 / 09844



Bescheinigung

ESU

| | |
|-------------------|-----|
| REC'D 15 FEB 2000 | |
| WIPO | PCT |

09/889420

Die Deutsche Telekom AG in Bonn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

„Einrichtung und Verfahren zur Synchronisation von Stromchiffrierern in ATM-Netzen“

am 18. Januar 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol H 04 L 12/56 der Internationalen Patentklassifikation erhalten.

München, den 18. November 1999
Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Wehner



Aktenzeichen: 199 01 666.6

A 9161
06.90
11/98

(EUV-4)

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

BEST AVAILABLE COPY

Einrichtung und Verfahren zur Synchronisation von Stromchiffrierern in ATM-Netzen

Beschreibung

Die Erfindung betrifft eine Einrichtung und ein Verfahren zur Synchronisation mindestens eines Stromdechiffrierers, der empfängerseitig an einen Übertragungskanal für ATM-Zellen angeschlossen ist, mit einem senderseitig am Übertragungskanal angeordneten Stromchiffrierer, wobei Stromchiffrierer und Stromdechiffrierer jeweils einen Pseudo-Random-Generator aufweisen, der mit Hilfe eines geheimen Schlüssels einen variablen sender- und empfängerseitig gleichen Schlüsselstrom erzeugt.

Im Breitband-ISDN erfolgt die Übertragung im asynchronen Transfer-Modus (ATM), wobei die Informationen in Pakete gleicher Länge verpackt sind, sogenannte ATM-Zellen, im folgenden auch Zellen genannt. Eine Zelle besteht aus einem fünf Oktett großen Kopffeld (Header) und einem 48 Oktett großen Informationsfeld, das die Nutzlast (Payload) beinhaltet. Der Kopf der Zelle dient hauptsächlich zur Kennzeichnung der Verbindung, zu der diese Zelle gehört. Diese Kennzeichnung wird als Virtual Path Identifier (VPI) und Virtual Channel Identifier (VCI) bezeichnet. Diese und andere Informationen belegen im Kopffeld insgesamt 32 Bit und werden durch einen Acht-Bit-Fehlerkorrekturcode geschützt.

Dieser Fehlerkorrekturcode - auch HEC (Header Error Control) genannt - kann bis zu Drei-Bit-Fehler erkennen und Ein-Bit-Fehler und benachbarte Doppelfehler korrigieren. Außer zum Fehlerschutz wird der HEC auch zur Zellgrenzerkennung genutzt, was unter anderem in Sigmund: "ATM - Die Technik des Breitband-ISDN", R.v. Decker Verlag, 2. Auflage 1994.

Ein gültiges Kopffeld wird gefunden, wenn sich die aus diesen 32 Bit berechnete Prüfsequenz mit der im HEC-Feld übertragenen Prüfsequenz deckt. Die empfängerseitige Synchronisation rastet dann ein. Nach 53 Oktett wird wieder ein gültiges Kopffeld erwartet. Um den Prozeß der Zellgrenzerkennung nicht zu unterbrechen und somit die ATM-Zellsynchronisation zu erhalten, ist ein kontinuierlicher Zellenstrom erforderlich. Die ATM-Zellgrenzerkennung ist ein sehr robustes Synchronisations-Verfahren.

Bei Stromchiffrierern und Stromdechiffrierern wird eine von einem kryptographisch starken Pseudo-Random-Generator (PRG) erzeugte Pseudo-Zufallssequenz als variabler Schlüssel verwendet. Den unverschlüsselten Daten $p(t)$ wird der variable Schlüssel $k(t)$ modulo 2 aufaddiert. Das Ergebnis ergibt dann die verschlüsselten Daten $c(t)$. Mit dem gleichen variablen Schlüssel $k(t)$ erfolgt dann wiederum die Entschlüsselung. Damit jeweils der gleiche variable Schlüssel erzeugt wird, ist eine Synchronisation beider Pseudo-Random-Generatoren erforderlich.

Die Anwendung von Stromchiffrierern und Stromdechiffrierern in einem ATM-Netz und deren Synchronisation ist durch Heister U., Killat U.: "Private and Authentic Communication in Passive Optical Networks", International Journal of Network Management, Volume 5, Number 2, March-April 1995 beschrieben. Dabei wird zur Synchronisation des Stromdechiffrierers die Übertragung eines Initialisierungs-Vektors vorgeschlagen. Dies erfordert jedoch zusätzliche Übertragungskapazität.

Aufgabe der Erfindung ist es, ein zuverlässiges Verfahren zur Synchronisation von Stromdechiffrierern anzugeben, das keine zusätzliche Kapazität benötigt und mit möglichst geringem Aufwand zu implementieren ist.

Diese Aufgabe wird bei der erfindungsgemäßen Einrichtung dadurch gelöst, daß dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer jeweils ein Zustandsautomat zugeordnet ist, der von ATM-Zelle zu ATM-Zelle weiterschaltbar ist und wobei der jeweilige Zustand neben dem geheimen Schlüssel zur Bildung des variablen Schlüssels dient.

Bei einer bevorzugten Ausführungsbeispiel kann dabei vorgesehen sein, daß der Zustand einer Einrichtung zur Bildung einer Funktion in Abhängigkeit vom Zustand und dem geheimen Schlüssel zuführbar ist, die zur Steuerung des Pseudo-Random-Generators ausgebildet ist.

Die erfindungsgemäße Einrichtung kann sowohl zwischen optischen Leitungsanschlüssen (OLT = Optical Line Termination) als auch bei optischen Netzabschlüssen (ONT = Optical Network Termination) angewendet werden, wobei jeweils ein OLT und ein ONT über einen Pseudo-Random-Generator und einen Zustandsautomaten verfügen. Die Zustandsautomaten werden bei der Initialisierung des Systems alle in den gleichen Anfangszustand gesetzt. Jeder ONT hat einen geheimen Schlüssel.

Die erfindungsgemäße Einrichtung kann an sich auch bereits bei einer Übertragung zwischen einem Sender und einem Empfänger angewendet werden. Besonders vorteilhaft ist jedoch eine Weiterbildung, die darin besteht, daß beim Stromchiffrierer zur Bildung des variablen Schlüssels der geheime Schlüssel des Ziels der jeweils gesendeten ATM-Zelle und der jeweilige Zustand dient und die Zustandsautomaten des Stromchiffrierers und der Stromdechiffrierer unabhängig von dem Ziel der jeweiligen ATM-Zelle weiterschaltbar sind. Hierbei hat jeder ONT (Optical Network Termination) einen geheimen Schlüssel, der OLT (Optical Line Termination) die geheimen Schlüssel aller ONTs.

Bei dem erfindungsgemäßen Verfahren wird die Aufgabe dadurch gelöst, daß der variable Schlüssel ferner vom Zustand eines dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer zugeordneten Zustandsautomaten abhängt, der von ATM-Zelle zu ATM-Zelle weitergeschaltet wird. Dabei ist vorzugsweise vorgesehen, daß die Weiterschaltung des Zustandsautomaten bei Erkennen einer Zellgrenze durch Vergleich einer aus dem Kopffeld berechneten Prüfsequenz mit einer ebenfalls im Kopffeld der Zelle übertragenen Prüfsequenz abgeleitet wird. Dies bedeutet keinen Mehraufwand, da Einrichtungen zur Zellgrenzerkennung in den Empfängern ohnehin benötigt werden.

Eine vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens besteht darin, daß aus dem geheimen Schlüssel und dem jeweiligen Zustand mit Hilfe einer vorgegebenen Funktion eine Eingangsgröße für den jeweiligen Pseudo-Random-Generator gebildet wird.

Besonders vorteilhaft ist das erfindungsgemäße Verfahren, wenn an den Übertragungskanal mehrere Empfänger mit jeweils einem Stromdechiffrierer angeschlossen sind und wobei Kopffelder der ATM-Zellen Informationen darüber enthalten, welche Empfänger die ATM-Zellen zum Ziel haben, dadurch, daß der Bildung des variablen Schlüssels im Stromchiffrierer der geheime Schlüssel des Stromdechiffrierers am jeweiligen Ziel zugrundegelegt wird und daß die dem Stromchiffrierer und den Stromdechiffrierern zugeordneten Zustandsautomaten bei jeder übertragenen ATM-Zelle weitergeschaltet werden.

Ausführungsbeispiele der Erfindung sind in der Zeichnung anhand mehrerer Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 einen Ausschnitt aus einem ATM-Netz mit einem Sender und zwei Empfängern und

Fig. 2 eine schematische Darstellung eines an sich bekannten Verfahrens zur Zellgrenzerkennung.

In Fig. 1 sendet ein Sender 1, der Teil eines ansonsten nicht näher dargestellten OLT ist, einen Strom von ATM-Zellen über ein optisches Netzwerk 2 an Empfänger in ONTs, von denen lediglich zwei Empfänger 3, 4 dargestellt sind. Vor der Übertragung werden die Nutzdaten einer jeden Zelle mit einem Stromchiffrierer verschlüsselt, der aus einer Exklusiv-Oder-Schaltung 5 und einem Pseudo-Random-Generator 6 besteht, welcher der Exklusiv-Oder-Schaltung 5 jeweils einen variablen Schlüssel $k_1(t)$, $k_2(t)$ zuführt, so daß die Nutzdaten $p(t)$ als verschlüsselte Daten $c(t)$ zum optischen Netzwerk 2 geleitet werden. Zum Entschlüsseln sind den Empfängern 3 und 4 Stromdechiffrierer 7, 11; 8, 12 vorgeschaltet, zu welchen der Zellstrom jeweils über eine Einrichtung 9, 10 zur Erkennung der Zellgrenzen geführt wird und in denen je ein Pseudo-Random-Generator 11, 12 einen variablen Schlüssel $k_1(t)$, $k_2(t)$ ableitet, der je einer Exklusiv-Oder-Schaltung zugeleitet wird. Das von den Einrichtungen 9, 10 abgeleitete Signal zeigt die Grenze einer Zelle an und wird auch in den Empfängern 3, 4 zur Auswertung des Kopffeldes benötigt.

Eine Einrichtung zur Zellgrenzerkennung ist in Fig. 2 schematisch dargestellt, wobei aus dem über 2 zugeführten Zellstrom jeweils 40 Bit abgegriffen werden (in der Figur steht ein Pfeil für 4 Bit). Über die Bits 9 bis 40 wird bei 13 in gleicher Weise wie beim Sender ein HEC gebildet, der in einem 8-Bit-Vergleich 14 mit den vorangegangenen Bits 1 bis 8 verglichen wird. Bei Gleichheit wird bei 15 ein Signal abgegeben, das das Erkennen eines gültigen Kopffeldes bedeutet.

Dem Stromchiffrierer und den Stromdechiffrierern ist jeweils ein Zustandsautomat 16, 17, 18 zugeordnet, der zu Beginn jeder Zelle weitergeschaltet wird. Der dann jeweils eingenommene Zustand wird jeweils einer Einrichtung 19, 20, 21 zur Berechnung von Funktionswerten aus dem Zustand und einem geheimen Schlüssel zugeführt. Die Einrichtung 19 wird von dem Sender 1 derart gesteuert, daß je nach Ziel der Zelle ein geheimer Schlüssel k_1 oder k_2 angewendet wird. Die empfängerseitigen Einrichtungen 20 und 21 sind jeweils nur mit einem geheimen Schlüssel k_1 bzw. k_2 beaufschlagt.

Durch die Verschlüsselung mit dem Schlüssel des jeweiligen Empfängers und die Weiterschaltung der Zustandsautomaten 16, 17, 18 bei der Übertragung jeder Zelle wird an dem jeweiligen Empfänger immer der richtige variable Schlüssel $k_1(t)$ bzw. $k_2(t)$ angewendet. Die zur Synchronisation benutzte ATM-Zellgrenzerkennung ist ein sehr robustes Synchronisationsverfahren, das durch die Erfindung eine zuverlässige Dechiffrierung der übertragenen Daten ermöglicht.

Patentansprüche

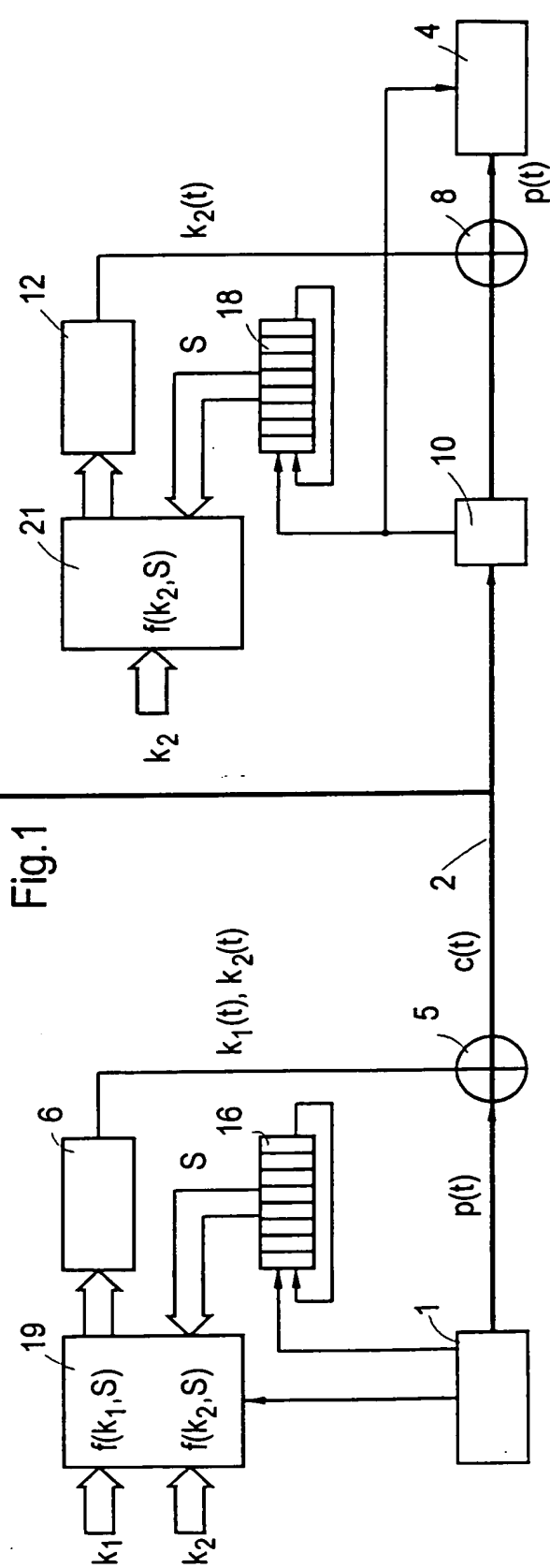
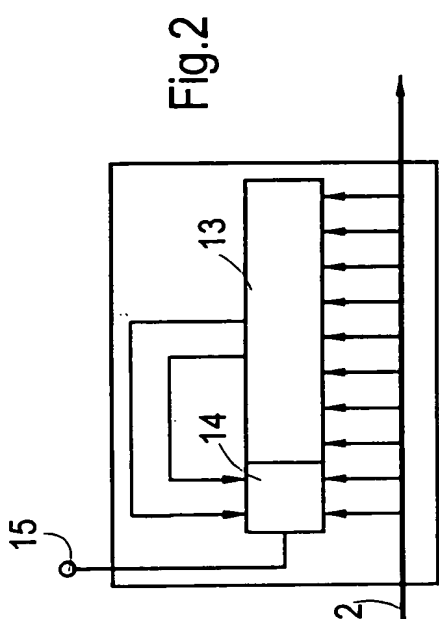
1. Einrichtung zur Synchronisation mindestens eines Stromdechiffrierers, der empfängerseitig an einen Übertragungskanal für ATM-Zellen angeschlossen ist, mit einem senderseitig am Übertragungskanal angeordneten Stromchiffrierer, wobei Stromchiffrierer und Stromdechiffrierer jeweils einen Pseudo-Random-Generator aufweisen, der mit Hilfe eines geheimen Schlüssels einen variablen sender- und empfängerseitig gleichen Schlüssel erzeugt, dadurch gekennzeichnet, daß dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer jeweils eine Einrichtung zur Zellgrenzerkennung und ein Zustandsautomat zugeordnet ist, wobei der Zustandsautomat von der Einrichtung zur Zellgrenzerkennung weiterschaltbar ist und der jeweilige Zustand neben dem geheimen Schlüssel zur Bildung des variablen Schlüssels dient.
2. Einrichtung nach Anspruch 1, dadurch gekennzeichnet, daß der Zustand einer Einrichtung zur Bildung einer Funktion in Abhängigkeit vom Zustand und dem geheimen Schlüssel zuführbar ist, die zur Steuerung des Pseudo-Random-Generators ausgebildet ist.
3. Einrichtung nach einem der vorhergehenden Ansprüche, wobei an den Übertragungskanal mehrere Empfänger mit jeweils einem Stromdechiffrierer angeschlossen sind und wobei Kopffelder der ATM-Zellen Informationen darüber enthalten, welche Empfänger die ATM-Zellen zum Ziel haben, dadurch gekennzeichnet, daß beim Stromchiffrierer zur Bildung des variablen Schlüssels der geheime Schlüssel des Ziels der jeweils gesendeten ATM-Zelle und der jeweilige Zustand dient und die Zustandsautomaten des Stromchiffrierers und der Stromdechiffrierer unabhängig von dem Ziel der jeweiligen Zelle weiterschaltbar sind.

4. Verfahren zur Synchronisation mindestens eines Stromdechiffrierers, der empfängerseitig an einen Übertragungskanal für ATM-Zellen angeschlossen ist, mit einem senderseitig am Übertragungskanal angeordneten Stromchiffrierer, wobei Stromchiffrierer und Stromdechiffrierer jeweils einen Pseudo-Random-Generator aufweisen, der mit Hilfe eines geheimen Schlüssels einen variablen sender- und empfängerseitig gleichen Schlüssel erzeugt, dadurch gekennzeichnet, daß der variable Schlüssel ferner vom Zustand eines dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer zugeordneten Zustandsautomaten abhängt, der von ATM-Zelle zu ATM-Zelle weitergeschaltet wird.
5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Weiterschaltung des Zustandsautomaten bei Erkennen einer Zellgrenze durch Vergleich einer aus dem Kopffeld berechneten Prüfsequenz mit einer ebenfalls im Kopffeld der Zelle übertragenen Prüfsequenz abgeleitet wird.
6. Verfahren nach einem der Ansprüche 4 oder 5, dadurch gekennzeichnet, daß aus dem geheimen Schlüssel und dem jeweiligen Zustand mit Hilfe einer vorgegebenen Funktion eine Eingangsgröße für den jeweiligen Pseudo-Random-Generator gebildet wird.
7. Verfahren nach einem der Ansprüche 4 bis 6, wobei an den Übertragungskanal mehrere Empfänger mit jeweils einem Stromdechiffrierer angeschlossen sind und wobei Kopffelder der ATM-Zellen Informationen darüber enthalten, welche Empfänger die ATM-Zellen zum Ziel haben, dadurch gekennzeichnet, daß der Bildung des variablen Schlüssels im Stromchiffrierer der geheime Schlüssel des Stromdechiffrierers am jeweiligen Ziel zugrundegelegt wird und daß die dem Stromchiffrierer und den Stromdechiffrierern zugeordneten Zustandsautomaten bei jeder übertragenen ATM-Zelle weitergeschaltet werden.

Zusammenfassung

Bei einer Einrichtung und einem Verfahren zur Synchronisation mindestens eines Stromdechiffrierers, der empfängerseitig an einen Übertragungskanal für ATM-Zellen angeschlossen ist, mit einem senderseitig am Übertragungskanal angeordneten Stromchiffrierer, wobei Stromchiffrierer und Stromdechiffrierer jeweils einen Pseudo-Random-Generator aufweisen, der mit Hilfe eines geheimen Schlüssels einen variablen sender- und empfängerseitig gleichen Schlüssel erzeugt, ist dem Stromchiffrierer und dem mindestens einen Stromdechiffrierer jeweils eine Einrichtung zur Zellgrenzerkennung und ein Zustandsautomat zugeordnet, wobei der Zustandsautomat von der Einrichtung zur Zellgrenzerkennung weiterschaltbar ist und der jeweilige Zustand neben dem geheimen Schlüssel zur Bildung des variablen Schlüssels dient.

1/1



This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

